Dr. Markus Böhm

ist Partner bei PricewaterhouseCoopers in Frankfurt und dort verantwortlich für IT-Governance, Risikomanagement und Compliance. Zuvor hat er in Informatik promoviert, ist Autor vieler Fachbeiträge zu diesen Themen und hat auch einen Lehrauftrag.

Eiko Ermold

ist Enterprise IT Architect bei PricewaterhouseCoopers AG WPG in Frankfurt. Nach einigen Jahren, in den Bereichen Risk-Management und der prüfungsnahen IT-Beratung, erfolgte ein Wechsel zur internen IT in den Bereich IT Strategy & Security als Enterprise IT Architect. Akademischer Hintergrund: Studium der Betriebswirtschaft an der Universität Gießen.

Dr. Axel Kessler

LL.M., ist innerhalb der Rechtsabteilung der Siemens AG u. a. für IT-rechtliche Fragestellungen zuständig, einschließlich Datenschutz, regulatorische Themen und allgemeines Vertragsrecht.

Heino Wehran

ist Wirtschaftsprüfer und Steuerberater und bei der PricewaterhouseCoopers AG WPG seit über 10 Jahren in der Beratung zu Aufbau und Optimierung sowie in der Prüfung von Compliance Management Systemen tätig. Sein besonderer Schwerpunkt betrifft die praktische Umsetzung von Compliance bei komplexen Prozessen und IT-Systemen.

Markus Vehlow

arbeitet seit mehr als zehn Jahren bei PricewaterhouseCoopers in Frankfurt am Main und verantwortet bei PwC das Thema Cloud Computing in Deutschland und Österreich. Zudem hat er zahlreiche Artikel und Fachbeiträge zum Thema Cloud Computing verfasst und ist Autor zweier Cloud-Studien (Anbieterstudie „Navigation in der Wolke" und Nutzerstudie „Cloud Computing im Mittelstand").

Compliance und Cloud Computing – IT-Compliance-Anforderungen an Cloud Computing

(Auszüge aus dem BITKOM-Leitfaden „Cloud Computing – Was Entscheider wissen müssen")

Die individuellen Rahmenbedingungen eines Unternehmens, die sowohl den Nutzer von Cloud Computing als auch dessen Anbieter betreffen, führen zu unterschiedlichen Anforderungen an die IT-Compliance. Von Bedeutung sind hierbei unter anderem die Branche, die Rechtsform, der Ort der Unternehmung bzw. der Leistungserbringung oder die angebotenen Produkte und Dienstleistungen.

Diese Anforderungen betreffen in aller Regel nicht nur die IT des Anwenders selbst, sondern auch die von externen Anbietern beschafften (IT-)Dienstleistungen. Hierbei muss beachtet werden, dass zwar einzelne Aufgaben jederzeit an beliebige Dienstleister delegiert werden können, dass jedoch die Verantwortung zur Erfüllung dieser Anforderungen (und das Tragen der Konsequenzen bei Nichterfüllung) in aller Regel beim Auftraggeber und Nutzer der Dienste verbleibt.

Dieses Grundprinzip gilt sinngemäß auch für die Auslagerung von Aufgaben oder Prozessen in eine Cloud-Lösung. Für den Auftraggeber ist es daher wichtig herauszufinden, wo und wie seine IT insgesamt („innerhalb und außerhalb der Cloud") von den Anforderungen betroffen ist oder nicht. Die Tabelle zeigt beispielhaft eine vereinfachte Kategorisie-

rung von Anforderungen mit Bedeutung für IT-Compliance im Überblick.

Primär externe Vorgaben		Primär interne Vorgaben	
Gesetzliche Regelungen	Externe Regelwerke	Interne Verpflichtungen	Verträge
SOX	GoBS	Ethik-Richtlinie (Code of Ethics)	Software-Lizenzverträge
HGB	GDPdU	IT-Einkaufsrichtlinie	Outsourcing-Verträge (SLA)
KonTraG	ISO 20000	E-Mail-Richtlinie	Wartungsverträge
EG Dual Use	ISO 38500	Richtlinie zur Internetnutzung	Verträge zur Geheimhaltung
...	...	...	...

Tab.: Beispielhafte Kategorisierung von IT-Compliance-Anforderungen

Auf Basis vergleichbarer Überlegungen kann ein Unternehmen die jeweilige Relevanz der einzelnen Anforderungen überprüfen und erforderlichenfalls weitere Schritte zur Umsetzung seiner IT-Compliance-Maßnahmen planen.

Im Hinblick auf Cloud Computing insgesamt ist dabei festzuhalten, dass für Cloud Computing dem Grunde nach die bisher bekannten Anforderungen gelten. Cloud-Computing-Anforderungen unterscheiden sich also nicht von den allgemeinen IT-Compliance-Anforderungen.

Weiterhin ist darauf hinzuweisen, dass sich die IT-Compliance-Anforderungen im Prinzip in jedem Fall auf die allgemeinen Ziele zur adäquaten Behandlung von IT-Risiken reduzieren lassen. Dies können im Einzelnen insbesondere Sicherheit, Verfügbarkeit, Vollständigkeit und Nachvollziehbarkeit etc. sein.

Gesetzliche Regelungen

Auch Gesetze, deren Namen und Inhalt nicht sofort mit IT in Zusammenhang gebracht wird, enthalten nicht selten Einzelanforderungen im Sinne von IT-Compliance. Eine besondere (zweifelhafte) „Berühmtheit" hat hierzu in den letzten Jahren der viel zitierte Sarbanes Oxley-Act erlangt (Die im Zusammenhang mit dem Sarbanes Oxley-Act in den USA getroffenen Regelungen sollen die Integrität, Vollständigkeit und Korrektheit der Daten für die Finanzberichterstattung unterstützen).

Nun hat dieser Leitfaden nicht die Aufgabe, alle denkbaren Compliance-Anforderungen ausführlich darzustellen. Vor diesem Hintergrund werden nachfolgend exemplarisch grundlegende handelsrechtliche bzw. steuerrechtliche Aspekte allgemein dargestellt. Darüber hinaus wird als gesondertes Einzelbeispiel die Dual-Use-Verordnung im Zusammenhang mit exportwirtschaftlichen Fragestellungen zur Veranschaulichung weiter ausgeführt.

Für externe Interessenten allgemein, aber insbesondere auch für die Finanzverwaltung, bilden die Abschlüsse und Finanzinformationen eines Unternehmens eine wesentliche Informationsquelle. Die Finanzberichterstattung folgt daher strengen Regeln und unterliegt zum Teil der externen Überprüfung und Überwachung.

Betroffen sind von diesen Regeln im Prinzip alle Aktivitäten, die einen Einfluss darauf haben, wie Unternehmenstransaktionen initiiert, aufgezeichnet, verarbeitet und berichtet werden. Hierzu genügt es, dass diese Aktivitäten direkt oder indirekt die Vermögens-, Finanz- oder Ertragslage eines Unternehmens beeinflussen. Beispiele für solche Aktivitäten sind Produktion, Lagerhaltung, Logistik oder die Lohn- und Gehaltsabrechnung. In unmittelbarer Folge sind auch die unterstützenden IT-Aktivitäten von damit verbundenen Anforderungen betroffen. Der damit beispielsweise seitens der Finanzverwaltung verbundene Grundgedanke lässt sich in wenigen Schritten darstellen: Korrekte und verlässliche Finanzdaten können nur dann sichergestellt werden, wenn

- im Zuge ihrer Erstellung, Verarbeitung und Darstellung auch in der IT keine Möglichkeiten zur Verfälschung gegeben sind,
- dennoch (im Zusammenhang mit der IT) auftretende Fehler erkannt und behoben werden,
- allgemein die Sicherheit und Verfügbarkeit der IT-Systeme gewährleistet ist und
- die Nutzung der IT bestimmten allgemeinen Grundregeln unterliegt.

Um dieses Ziel zu unterstützen, wurden eine Reihe von Präzisierungen für IT-Compliance-Anforderungen definiert (vgl. auch nächster Abschnitt). Diese betreffen umfangreiche Einzelregelungen zum Einsatz der IT im Unternehmen wie beispielsweise in den Bereichen IT-Umfeld, Informationssicherheit, Programmentwicklung, Programmpflege und IT-Betrieb.

Das Besondere an diesen Anforderungen im Zusammenhang mit Cloud Computing liegt darin, dass vor allem die Finanzverwaltung ein hohes Interesse daran hat, dass die Daten sicher und geschützt vor nicht autorisierten Änderungen verarbeitet werden. Wesentlich in diesem Zusammenhang ist auch die Frage der Verfügbarkeit für die Finanzverwaltung. Daher unterliegt eine Datenverarbeitung im Ausland für steuerliche Zwecke gesonderten Auflagen und Anforderungen.

Das zweite konkrete Einzelbeispiel bilden allgemeine exportkontrollrechtliche Bestimmungen (EG-Dual-Use-Verordnung). Auch diese sind im Hinblick auf IT-Compliance-Anforderungen zu berücksichtigen.

Dabei ist zu beachten, dass der nichtphysische Transfer von Daten, Technologie und Software im Prinzip den gleichen exportkontrollrechtlichen Beschränkungen wie der physische Transfer von Gütern unterliegt. Entsprechend müssen die zu transferierenden Daten vor dem Zugriff durch sanktionierte („gelistete") Personen, Unternehmen und Organisationen geschützt werden. Gleichzeitig müssen etwaige Beschränkungen für den Transfer von Daten beachtet werden, die an verschiedene Faktoren (Art der Daten, Verwendungszweck der Daten, Standort der Server, Nationalität der beteiligten Personen mit Zugriffsmöglichkeit) anknüpfen. Die Beschränkungen gelten in erster Linie, aber nicht ausschließlich, für den grenzüberschreitenden Datentransfer. Bereits die bloße Zugriffsmöglichkeit durch einen ausländischen Administrator oder eine anderweitig beteiligte ausländische Person per se kann als Export im Sinne dieser Vorschriften gewertet werden.

Die Umsetzung der exportkontrollgesetzlichen Vorgaben wird (schon unabhängig von den besonderen Aspekten des Cloud Computing) dadurch erschwert, dass die exportkontrollrechtlich kritischen Daten häufig in verschiedenen Systemen und Anwendungen integriert sind, sodass eine Identifikation und Isolation dieser Daten einen sehr hohen Aufwand bedeuten. Hierzu bedarf es der Definition klarer Prozesse zur Selektion entsprechend der exportkontrollrechtlichen Relevanz.

Externe Regelwerke

Externe Regelwerke können in Form von Richtlinien und allgemeinen Standards auftreten. Exemplarisch zu nennen sind in Fortsetzung des Beispiels die „Grundsätze ordnungsmäßiger DV-gestützter Buchfüh-

rungssysteme“ (GoBS) oder die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (GDPdU). Beide Regelungen unterstützen letztlich die Durchsetzung des Steueranspruchs durch die Finanzverwaltung, indem konkrete Vorgaben bezüglich Art und Inhalt der Datenverarbeitung im Umfeld von Buchführungssystemen gegeben werden.

Auch privatrechtliche Institutionen können externe Regelwerke (meistens als allgemeine Qualitätsstandards und/oder „Good Practice“) erarbeiten. Hierzu zählen beispielsweise das Deutsche Institut für Normung (DIN) oder die International Organization for Standardization (ISO). Von der ISO entwickelte Standards umfassen unter anderem die ISO/IEC 20000 (IT Service Management) oder die ISO/IEC 38500 (Corporate Governance of Information Technology). Solche Standards sind rechtlich zunächst nicht verpflichtend. Dies gilt zumindest solange, wie sie nicht konkret in einzelne Rechtsnormen aufgenommen wurden. Unabhängig davon können sie aber jederzeit zivilrechtlich zwischen einzelnen Vertragsparteien gesondert vereinbart werden.

Etablierte Standards können bei wachsender Verbreitung und Akzeptanz als „Stand der Technik“ oder „übliche Berufsauffassung“ angesehen werden. Dies hat zur Folge, dass über allgemeine Grundsätze einer ordnungsgemäßen Geschäftsführung zumindest eine indirekte Verpflichtung zur Einhaltung entstehen kann. Einer derartigen Verpflichtung kann dann wiederum in gerichtlichen Auseinandersetzungen besondere Bedeutung zukommen, wenn im Zusammenhang mit der Nichteinhaltung/Zuwiderhandlung Nachteile oder Schäden entstehen.

Interne Verpflichtungen und Verträge

Interne Verpflichtungen umfassen beispielsweise eigens definierte Unternehmensrichtlinien (z. B. für ethische Werte, den IT-Einkauf oder die Internet- bzw. E-Mail-Nutzung) zur Umsetzung der jeweils gewünschten Vorgaben.

Bei den Verträgen handelt es sich um alle Vereinbarungen, die mit Geschäftspartnern geschlossen wurden. Mögliche Geschäftspartner sind neben den eigenen Kunden natürlich auch Hersteller und Lieferanten von Hard- und Software, Anbieter von Dienstleistungen sowie sonstige Zulieferer in der Wertschöpfungskette des Unternehmens.

Da es sich bei den internen Verpflichtungen und Verträgen jeweils um sehr unterschiedliche und individuelle Inhalte handelt, wird hier auf eine detaillierte Darstellung verzichtet.

Ein für den Umgang mit Cloud Computing besonderer Punkt zeichnet sich aus den oben angeführten Beispielen ab: Die Anforderungen können aufgrund der Ausgestaltung des Cloud Computings eine besondere und bisher im Zweifel nicht oder nicht so umfassend beachtete Bedeutung erlangen. Dies wird deutlich, wenn es direkt oder indirekt um die Frage geht, in welchen Ländern die Daten gehalten bzw. verarbeitet werden, oder wenn die Frage betroffen ist, wie die Anbieter von Cloud Computing mit spezifischen Anforderungen zur Sicherheit und zum Datenschutz länderübergreifend umgehen.

Compliance-Risiken in der Cloud

Der Begriff „Risiko“ kann generell als das Produkt aus Eintrittswahrscheinlichkeit und Schadenshöhe bei Abweichung von einem angestrebten Zielzustand verstanden werden.

Der angestrebte Zielzustand ist die Erfüllung der Anforderungen aus externen und internen Regularien und Vorschriften. Die grundlegenden Anforderungen verändern sich auch bei Einsatz des Cloud Computings nicht.

Mithin stellt sich die Kernfrage, ob und inwieweit mit der Nutzung von Services aus der Cloud neue, bisher wenig oder nicht beachtete Risiken verbunden sind oder ob altbekannte Risiken angesichts der Cloud einer neuen Bewertung unterzogen werden müssen?

Ein Service aus der Cloud weist in der Regel „neue“ Merkmale auf, die in der bisherigen „klassischen“ IT nicht existieren. Dazu zählen u. a.

- der Applikationsbezug über das Internet,
- die hohe Virtualisierung sowie
- die Multi-Mandanten-Fähigkeit der Infrastruktur.

Einhergehend mit dieser Entwicklung müssen die Risiken neu bewertet werden.

Eine Virtualisierung der Betriebssysteme führt beispielsweise dazu, dass die Administratoren der Host-Systeme Zugriff auf die Gastsysteme haben können. Damit müssen die Maßnahmen, die bisher auf Betriebssystemebene für das Priviliged Account Management vorgesehen waren, auch auf die Betriebssystem-Virtualisierungsebene angewendet werden.

Ein anderes Beispiel: Wird der Cloud-Service aus dem Internet bezogen, so birgt der Ausfall der Internetverbindung ggf. ein besonderes Risiko für die Geschäftsprozesse des Unternehmens (bei für das Geschäft des Anwenders kritischen Komponenten). Damit sind die Maßnahmen, die bisher die geforderte Verfügbarkeit des lokalen Netzes sicherstellen sollten, analog auch auf die Internetanbindung anzuwenden. Ergänzend kommen neue Risiken hinzu, die nur indirekt mit dem Ausfall von beteiligten Komponenten in Verbindung stehen. So können besondere Internetdienste, auch wenn es sich „nur“ um das Live-Streaming während einer Fußball-Weltmeisterschaft handelt, die Internetverbindung so stark auslasten, dass ein Cloud-Service beeinträchtigt wird. Hier sind ggf. risikominimierende Maßnahmen zu treffen, die neu sind im Vergleich zu den Maßnahmen in der klassischen IT.

Anderseits dürfte das Verfügbarkeitsrisiko aufgrund von beispielsweise Festplattendefekten einzelner Server bei Bezug eines Services aus der Cloud tendenziell sinken (zumindest ist zu erwarten, dass die Service-Provider hierfür entsprechend Vorsorge getroffen haben).

Diese vereinfachten Beispiele zu den Risiken des Bezugs von Services aus der Cloud zeigen, dass verschiedene Arten von Risiken betrachtet werden müssen, um über geeignete Maßnahmen eine anforderungsgerechte Cloud-Dienstleistung (und damit die Cloud Compliance) sicherzustellen.

Im Einzelnen lassen sich diese Risiken, jeweils im Vergleich zu bisherigen „klassischen“ IT-Lösungen, wie folgt kategorisieren:

- gleichbleibende oder erhöhte Risiken, die ein neues Cloud-Merkmal betreffen, denen mit analogen Maßnahmen begegnet werden kann (z. B. Privileged Accounts auf einer Virtual Storage Management Station).
- neue Risiken, denen mit neuen Maßnahmen begegnet werden muss (z. B. Internet-Auslastung).
- tendenziell eher reduzierte Risiken, da die Infrastrukturelemente beispielsweise als Service und nicht als Hardwarekomponente eingekauft werden (z. B. Ausfall einer Festplatte).

Um einschätzen zu können, welche Risiken Cloud-Umgebungen in der spezifi-

schen Ebene (IaaS, PaaS, SaaS) und Organisationsform (Private, Hybrid, Public) mit sich bringen, sind sowohl eine detaillierte Analyse des zu beziehenden Service und aller genutzten Komponenten, als auch die Kenntnis über die neuen Cloud-Merkmale notwendig.

Diese umfassende Risikobetrachtung ist erforderlich, um anschließend Maßnahmen zu ergreifen und somit den Anforderungen zu genügen. Die Komplexität der Risikoanalyse sollte hierbei nicht unterschätzt werden.

Grenzen zur Erreichung von Cloud Compliance

Auch bei Beachtung aller Hinweise in den bisherigen Ausführungen können Situationen nicht ausgeschlossen werden, in denen Cloud Compliance nur mit unverhältnismäßigem Aufwand oder gar nicht erreicht werden kann:

- Im Zuge von Cloud-Diensten können Prozessverantwortliche ihre Prozesse zukünftig dank Service-orientierter Architekturen ohne Beteiligung der IT-Abteilung konfigurieren und anpassen.
- Die mit der Serviceorientierung verbundene Orchestrierung kann dazu führen, dass sich Cloud-Services unterschiedlicher Anbieter flexibel und beliebig lange in eine bestimmte Prozessaktivität integrieren lassen. Ein Anbieterwechsel könnte somit mehrmals im Monat geschehen.
- Zudem könnten sich das Prozessdesign und die damit verbundenen Prozessaktivitäten ständig ändern, was aus Sicht der Kunden zu ständig wechselnden Risikosituationen führen kann. Neuere Systeme zur Warenwirtschaft und Unternehmensplanung sind hierzu bereits in der Lage.
- Die Entscheidung darüber, welcher Provider zu welchem Prozessschritt genutzt wird, könnte agentenbasiert auf einem Cloud-Marktplatz gefällt werden. Im Bereich Logistik gibt es das heute schon.
- Auch ein Dienste-Handel im Sinne einer Börse für Cloud-Services ist denkbar. Spezielle Service-Integratoren könnten sich hier bedienen und kombinierte Servicepakete als Dienstleistungen platzieren.
- Cloud Computing, wie in diesem Kapitel dargestellt, würde die gesamte Informationswirtschaft, ihre Technologien und das Business der Fachabteilungen nachhaltig verändern. An die IT-Compliance solcher Szenarien ist bisher noch gar nicht gedacht. Daher muss mit der Arbeit zur Lösung dieser Compliance-Herausforderungen rasch begonnen werden. Cloud-Anbieter, die derartige Möglichkeiten im Rahmen ihrer Service-Erbringung anbieten, sollten sich im Rahmen ihres Service-Designs bereits jetzt Gedanken darüber machen. ■

CLOUDCOMPUTING
Powered by BITKOM

Mehr Informationen und weitere Aspekte des Cloud Computing als Leitfaden finden Sie unter www.cloud-practice.de – eine Informationsplattform des BITKOM e.V.